(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
28 avril 2005 (28.04.2005)

PCT

(10) Numéro de publication internationale
WO 2005/038692 A2

(51) Classification internationale des brevets[7] : G06F 21/00

(21) Numéro de la demande internationale :
PCT/FR2004/002579

(22) Date de dépôt international :
12 octobre 2004 (12.10.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0312152 17 octobre 2003 (17.10.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **SAGEM SA** [FR/FR]; Le Ponant de Paris, 27 rue Leblanc, F-75015 PARIS (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **CARLIER, Vincent** [FR/FR]; 15 rue Buffon, F-91400 ORSAY (FR). **CHABANNE, Hervé** [FR/FR]; 48 rue de la Marne, F-78200 MANTES LA JOLIE (FR). **DOTTAX, Emmanuelle** [FR/FR]; 29 rue de la Fontaine au Roi, F-75011 PARIS (FR).

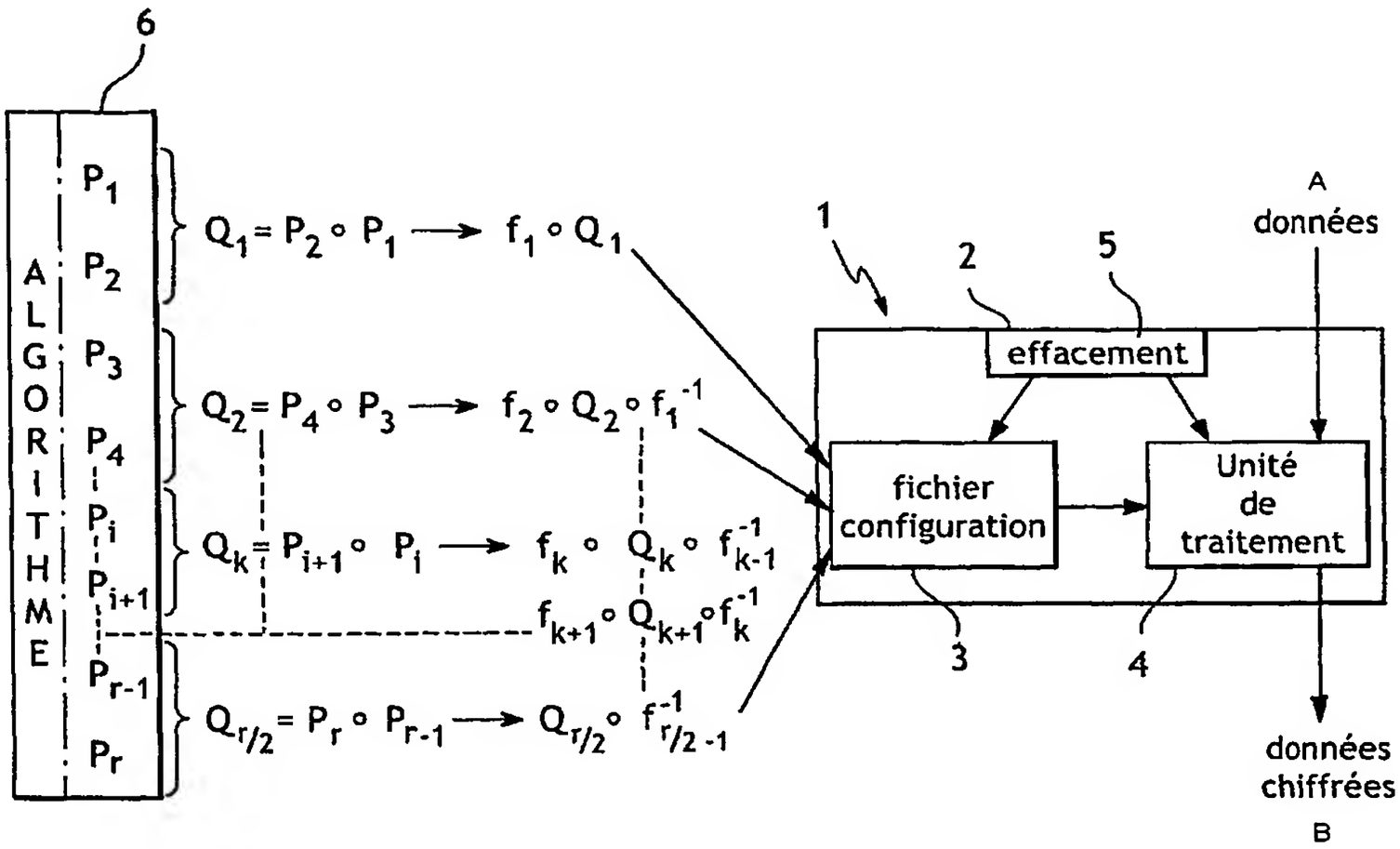
(74) Mandataires : **FRUCHARD, Guy** etc.; c/o CABINET BOETTCHER, 22 rue du Général Foy, F-75008 PARIS (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,

[Suite sur la page suivante]

(54) Title: METHOD FOR PROTECTION OF A CRYPTOGRAPHIC ALGORITHM

(54) Titre : PROCEDE DE PROTECTION D'UN ALGORITHME CRYPTOGRAPHIQUE



6 ALGORITHM
3 CONFIGURATION FILE
4 PROCESSING UNIT
2 ERASURE
A DATA
B CIPHERED DATA

(57) **Abstract:** The invention relates to a method for protection of a decomposable algorithm in the form of initial polynomials (P_i) with at least two variables and having a degree of at least two, comprises the steps of generation of combined polynomials (Q_k), each obtained from at least two initial polynomials (P_i, P_i+_1) and memorising the combined polynomials (Q_k) in the form of a configuration file in a memory (3), associated with a processing unit (4).

[Suite sur la page suivante]

WO 2005/038692 A2

PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Le procédé de protection d'un algorithme décomposable sous forme de polynômes initiaux (P_i) à au moins deux variables et ayant un degré au moins égal à deux, comporte les étapes de réaliser des polynômes combinés (Q_k) chacun obtenu à partir d'au moins deux polynômes initiaux (P_i, P_i+_1), et de mémoriser les polynômes combinés (Q_k) sous forme d'un fichier de configuration dans une mémoire (3) associée à une unité de traitement (4).